Prospective Management of Health IT Hazards

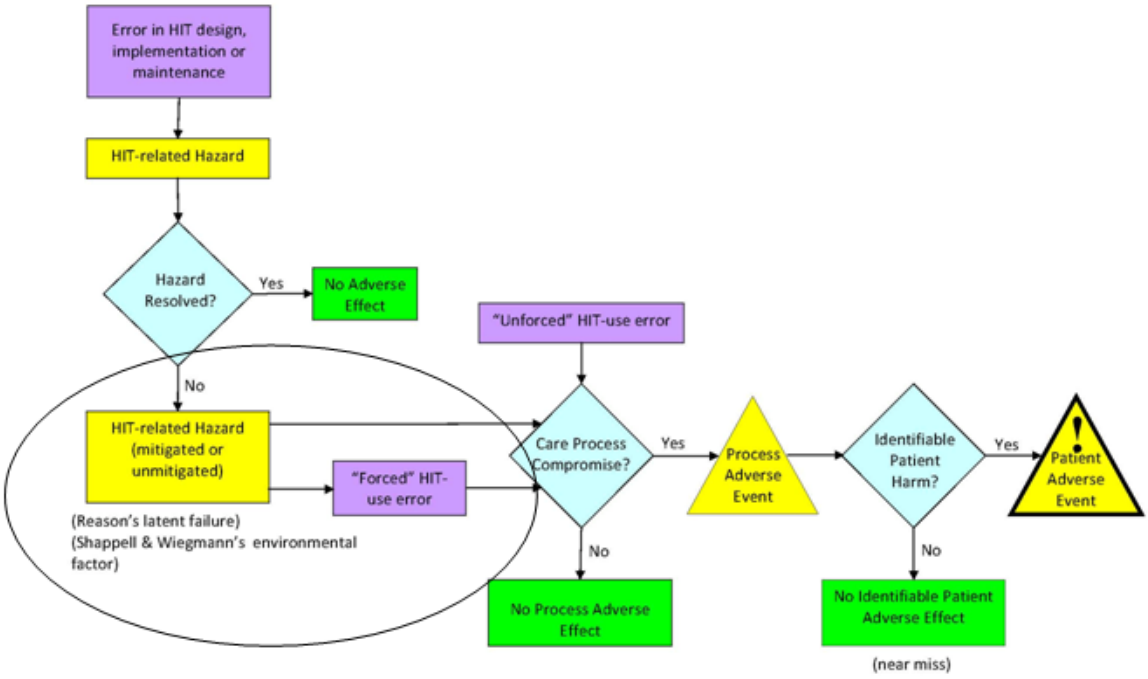
Executive Summary (case presentation)

In 2005, Geisinger was preparing for its first inpatient EHR implementation. Several months into the project, the project director informed the CIO and me that the EHR team's business analysts were unable to map safe and effective workflows between the new order-entry system and our existing pharmacy system (provided by another vendor). They and the project director believed that the only safe approach was to de-install the existing pharmacy system and replace it with the pharmacy system provided by the order-entry vendor—at a cost of several hundred thousand dollars and a nine months' delay in the project. Pharmacy's management was pained by the need to remove what was indisputably the best pharmacy system on the market (which they had used very effectively to improve safety and efficiency). Nevertheless, they agreed with the workflow analysis and supported the change. Executive leadership approved the change and we proceeded. Two years later (2007), when I reported this experience to an EHR-safety conference, David Classen noted that the results of the Leapfrog CPOE test in 62 carefully studied hospitals confirmed that this hazard (which was first noted in 2003) appears to be present regardless of which vendors' products are used. (Classen, in press)

This case illustrates several features of prospective hazard management (as opposed to an approach limited to retrospective analysis of HIT-related "near misses" and accidents):

- Importance of Hazards – As the Figure illustrates, resolving a hazard before it is implemented eliminates the risk that patients will be harmed due to it.

Figure. Prospective Hazard Management



- Impact on cost and speed of health IT implementation – Despite the high cost of resolving this hazard, the cost of resolving it after it had caused medication errors (care-process compromise) and user frustration would have been much higher—in direct IT costs and in even greater organizational costs. (More than one HCO has found that a serious problem with health IT implementation has made further adoption untenable for years afterward.)
- Difficulty - Prospective health IT hazard management requires highly skilled business analysts, healthcare informaticians, and IT leaders who have earned the trust of the organization. It depends on departmental and executive leaders who understand the strategic importance of health IT and are deeply committed to safety.
- "Reportability" – It is feasible for HCOs and vendors to discuss hazards (particularly those that have been successfully resolved) in a way that is not true of compromised care processes ("near misses") or patient harm.

- Need for effective dissemination – Knowledge of hazards such as this one has genuine potential to prevent patient harm and decrease healthcare costs. Such information needs to be widely available as rapidly as possible, particularly with the acceleration of health IT adoption efforts.
- Need for a common language and a usable tool – Effective hazard communication requires a common language and a useful tool for managing and communicating potential hazards.

Introduction

Organizations that implement and maintain EHRs and other health IT (HIT) carefully identify and manage hundreds of potential hazards annually—as part of the discipline that enables them to achieve significant improvements in care-process performance and patient outcomes. (Casale, 2007) For example, a hospital might plan to transmit prescriptions for post-discharge medications from its EHR to retail pharmacies electronically. Careful process analysis would reveal that retail pharmacies do not process electronically transmitted cancellations of prescriptions (even before they are received by the patient). More analysis might reveal that nurses frequently destroy printed prescriptions that have been superseded by physicians' new orders for post-discharge medications. Given these facts, electronic transmission of post-discharge medications would create a hazard that patients might receive dangerously redundant post-discharge medications.

Definitions

- Care-Process Compromise – Any change in a healthcare process that has the potential to cause patient (or caregiver) harm. ("Near misses" are a subset of care-process compromise that do not cause patient harm despite having significant potential to do so.)

- HCO (health care organization) – an organization that uses health IT to provide healthcare services to healthcare consumers

- Health IT Hazard - Any characteristic of health IT and its interactions with other healthcare systems that has the potential to contribute to adverse effects

- Health IT Effects
    - Positive Effects
        - Planned (benefits realized)
        - Unplanned (serendipity)*
    - Adverse Effects
        - Unresolved hazards (Reason's latent errors)
            - Anticipated and justified by risk-benefit analysis (trade-offs)
            - Anticipated and dismissed (active negligence)
            - Could have been anticipated, but were not (passive negligence)†
            - Could not reasonably have been anticipated†
        - Care-process compromise ("near miss")‡
        - Patient Harm ("accident")‡

** This form of positive effect is sometimes called an "unintended consequence".*
† These forms of unresolved hazards are often called "unintended consequences".
‡ These forms of adverse effect can result from anticipated or unanticipated unresolved hazards; they are often called "unintended consequences".

Despite the extensive experience of a few organizations in identifying, resolving, and monitoring HIT-related hazards and a small research literature focused on HIT-related "near misses" (care-process compromises) and patient harm, little is known (by researchers, vendors or implementers) about 1) the potential range and types of hazards associated with the use of health IT, 2) the likelihood that these hazards will contribute to patient harm, or 3) reliable methods for identifying and resolving HIT-

related hazards. Nor is there a standard terminology for characterizing health IT hazards and communicating them.

Hazard Control

Health IT safety begins with hazard control because many (perhaps most) care-process compromises (among which are "near misses") and instances of patient harm were a hazard first. As Nancy Leveson, the pre-eminent software safety engineer notes, "Hazard analysis is accident analysis before the accident." (Nancy Leveson, 2009)

As the Figure (above) illustrates, hazards arise due to failures in health IT design, implementation, and maintenance. (While many of these failures are due to a lack of skill or vigilance, many more are due to the interactions of complex healthcare processes and the necessary complexity of IT systems capable of supporting those processes.) If hazards are identified and resolved before implementation, no adverse effect can occur. If, however, the hazard is not identified or cannot be resolved, there is a risk that the hazard will overwhelm clinician vigilance and skill and cause or contribute to care-process compromise (and potentially patient harm). For example, if orders cannot be entered for a patient until the patient has arrived at the hospital, urgent care that otherwise would have been ordered during transport and ready to be initiated on arrival will be delayed, with potentially lethal effects. (Han, 2005)

The ability to prevent adverse effects is the reason Wogalter asserts that "Hazard control is critically important to the development and maintenance of safe products and services." (Wogalter, 2006) Focusing on hazards has other advantages. It changes a limited focus on "near misses" and accidents to a more systematic and productive focus on the hazardous characteristics of care systems, health IT, and their interactions. In addition, it calls attention to the work of other, critically important human actors, including care-process designers, software designers, coders, implementers (who fit health IT to the needs of users and processes), and those who maintain health IT over time.

Focusing on hazards prospectively also engages the skills and passion for quality of many of the most knowledgeable stakeholders in HIT safety promotion: healthcare informaticians, business analysts, clinicians, patients, safety teams, production-support teams, trainers, and software developers. From the perspective of cognitive psychology, prospective (non-emergent) hazard assessment gives these experts time to consider health IT safety from multiple perspectives in a setting that increases the likelihood of identifying previously unanticipated hazards. Finally, prospective hazard management reduces important forms of bias associated with retrospective analysis: hindsight, political, sponsor, and confirmation biases. (Johnson, 2007)

Prospective Hazard Management

"Hazard control consists of hazard analysis, elimination of hazards through design, guarding against hazards, removal of the product or service from use, warnings about the hazard, and training in hazard avoidance." (Wogalter, 2006) Additionally, hazard control includes reporting of hazards identified to other users and vendors.

In Geisinger's experience, hazard management takes all of these forms: Some hazards are resolved by vendor software fixes. In many cases, Geisinger programmers create fixes—although this introduces the potential for introducing hazards elsewhere in the software and entails extensive safety testing. When neither of these options is feasible, the "feature" is not implemented. Finally, when none of the preceding options is available, we train users carefully and monitor for adverse effects. Hazard communication is limited to direct communications with the vendor and personal contacts with a small number of HCOs and safety engineers.

Hazard Management Needs by Stakeholder

1. HCOs
    a. A usable tool for documenting hazard management from identification to resolution or mitigation (Uden-Holman, 1996)
    b. Reporting anonymity (Uden-Holman, 1996)

2. Health IT Customer Communities
    a. Share hazards and resolutions reported for the products they use.
    b. Customer confidentiality
3. Health IT Vendors
    a. Improve product usability and safety.
    b. Disseminate identified hazards and fixes to customers.
    c. Anonymity outside the customer community
4. Researchers, policy makers and the public
    a. Understand the variety, extent, and impact of HIT-related hazards and fixes.

Government Options

1. Fund annual systematic reviews of significant HIT-related hazards and fixes (such as the difficulty of interfacing pharmacy and order-entry systems).
2. Provide a tool to enable HCOs to manage potential hazards effectively (such as the HIT Hazard Manager™, Appendix A).
    a. Usability and usefulness will be critical.
    b. A comprehensive, task-appropriate terminology will support both. (See the Appendix.)
3. Enable automatic, anonymous reporting of potential hazards (including those that actually compromise a care-process and those that cause patient harm) under the protection of a Patient Safety Organization (PSO).
4. Require vendors to document prospective hazard management plans (that include timely communication of hazards and fixes to customers and a national clearinghouse)
5. Require HCOs to document prospective hazard management plans (that include timely communication of hazards to vendors and a national clearinghouse)

Potential effects on pace of health IT development and implementation

Enhanced identification, prevention, management, and reporting of HIT-related hazards have the potential to improve the quality and efficiency of care, including patient well being. (Wangsness, 2009) Improved knowledge regarding potential HIT-related hazards and how to resolve them would enable users of health IT to work more efficiently and create fewer hazards throughout the health IT life cycle (selection, configuration, training, and optimization). Vendors' design and quality-assurance efforts would be better informed, enabling them to avoid expensive emergency fixes to hazards identified in production systems. Easily accessible information on hazards could inform the development of innovative health IT that decreases the need for HCOs to perform extensive hazard control themselves, as is currently the case.

Requiring vendors to document prospective hazard management plans will accelerate market shake-out. Requiring HCOs to document such plans will increase the dependence of resource-constrained HCOs on providers of health IT solutions (bundled workflows and software).

References

Casale, A., et al. (2007). "ProvenCareSM: A Provider Driven Pay-for-Performance Program for Acute Episodic Cardiac Surgical Care." Ann Surg 246(4): 613-21.

Han, Y. Y., J. A. Carcillo, et al. (2005). "Unexpected Increased Mortality After Implementation of a Commercially Sold CPOE System." Pediatrics **116**: 1506-1512.

Israelski E.W., and W.H. Muto. (2007) "Human Factors Risk Management in Medical Products" Handbook of Human Factors and Ergonomics in Health Care and Patient Safety. P Carayon, ed. Lawrence Erlbaum Associates: Mahwah, NJ.

Johnson, J. and P. Barach (2007). Clinical Microsystems in Health Care: The Role of Human Factors in Shaping the Microsystem. Handbook of Human Factors and Ergonomics in Health Care and Patient Safety. P. Carayon. Mahwah, NJ, Lawrence Erlbaum Associates, Inc.

Leveson, N. (2009) personal communication

Uden-Holman, D. W. (1996). "Perceived barriers in reporting medication administration errors." Best Pract Benchmarking Health **1**: 191-97.

Wangsness, L. (2009). Beth Israel halts sending insurance data to Google: Hospital admits 'mistake' as flaws in practice found. Globe. Boston.

Wogalter, M.S. (2006) Purposes and Scope of Warnings in MS Wogalter, ed. Handbook of Warnings. Lawrence Erlbaum Associates, London.)

Appendix A

HIT Hazard Manager™

"An important first step in risk management is to understand and catalog the hazards and possible resulting harms that might be caused . . ." (Israelski, 2007) In consultation with nationally recognized healthcare informaticians, safety engineers, human-factors engineers, database designers, HIT vendors, and HCOs, Geisinger's EHR Safety Institute has designed and alpha tested the HIT Hazard Manager™, a tool for categorizing, managing, and reporting HIT-related hazards. The Hazard Manager is designed to be scalable for use as the infrastructure for a national clearinghouse of HIT-related hazards, care-process compromises, and occurrences of patient harm. Each provider organization contributing data to the clearinghouse would be able to 1) view and manage its own hazards confidentially, 2) view an aggregated set of hazards and fixes reported by other customers of its vendors and the vendor itself (with HCOs de-identified), and 3) view a complete set of hazards and fixes reported by all HCOs and vendors (de-identified to protect the anonymity of HCOs and vendors both). Similarly, each vendor could view all the hazards attributed to its products (with HCOs de-identified), in order to improve its products. Researchers and policy makers would be able to view all reported hazards and their effects (with HCOs and vendors de-identified).

Appendix B

Terminology of HIT-related Hazards

1. Discovery
    a. Stage of Discovery
        i. Software Specification
        ii. Vendor Programming
        iii. Customer Configuration
        iv. Customer Programming
        v. Testing
        vi. Training
        vii. Go-Live
        viii. Production Use
        ix. Upgrade
    b. Discovery Method
        i. Prospective Risk Analysis
        ii. Usability Testing
        iii. Electronic Report (Pre-Defined)
        iv. Error Log
        v. Chart Review
        vi. End-User Report
        vii. Retrospective Analysis (e.g., root-cause analysis)
    c. Discovered by
        i. End-User
        ii. Local IT
        iii. Local Medical Records
        iv. Safety Personnel
        v. Patient or Caregiver
        vi. HIT Vendor
        vii. 3rd-Party Content Vendor
        viii. Researcher
        ix. Regulator
    d. Publication method
        i. Internal Report (not published)
        ii. HIT Vendor Communication
        iii. 3rd-Party Content Vendor Communication
        iv. Healthcare Organization Communication (Listserv, User Group)
        v. Published Report (including electronic)

2. Causation
    a. Usability
        i. Difficult Information Access
        ii. Difficult Data Entry
        iii. Excessive Demands on Human Memory
        iv. Confusing Information Display

v. Inconsistent Information Display
vi. Mismatch between HIT function and clinical reality
vii. Inadequate or Confusing Feedback to the user
viii. Electronics-induced Credulity (excessive trust)

b. Data Quality
   i. Incorrect patient information
   ii. Information linked to the wrong patient
   iii. Faulty reference information
   iv. Miscalculation of a result (by HIT software)
   v. Lost data

c. Clinical-Decision Support
   i. Faulty Recommendation
   ii. Missing Recommendation
   iii. Clinical Content Inadequate
   iv. Decision-Engine Logic Inadequate
   v. Inappropriate level of automation

d. Software Design
   i. Faulty vendor implementation/configuration recommendation
   ii. Inadequate control of user access
   iii. Inadequate clinical content (including 3rd-party)
   iv. Unusable software-implementation tools
   v. Sub-optimal interfaces between applications

e. Implementation
   i. Inadequate software change control
   ii. Inadequate user-access control
   iii. Unpredictable elements of the patient's record available only on paper or as scanned documents

f. Hardware
   i. Insufficient hardware
   ii. Hardware poorly located
   iii. Hardware not working
   iv. Network not working
   v. Server not working
   vi. Slow response time

g. Non-HIT factors
   i. Individual
      1. Untrained User
      2. Fatigue
      3. Excessive workload (including cognitive)
      4. Unprofessional behavior
   ii. HCO
      1. Care processes poorly defined
      2. Unclear care policies

3. Inadequate project management
4. Inadequate human factors engineering
5. Inadequate change management
6. Inadequate training infrastructure

iii. Healthcare Sector
1. Complexity of healthcare
2. Reimbursement policies
3. Problematic data and communications standards
4. Regulatory requirements

h. Impact
i. Risk of care-process compromise
1. Ruled Out Definitively
2. Low likelihood
3. Moderate likelihood
4. High likelihood
5. Has occurred – Here
6. Has occurred – Elsewhere

ii. Type of care-process compromise
1. Delay in Care
2. Omission (inappropriate inaction)
3. Commission (inappropriate action)
4. Other, please specify.

iii. Potential for patient harm
1. Low
2. Medium
3. High

iv. Potential for healthcare professional harm
1. Low
2. Medium
3. High

v. Actual care-process compromise
1. Caught before it affected a patient
2. Did not affect a patient, despite not being caught
3. Affected a patient

vi. Actual patient harm
1. Harm Ruled Out Definitively
2. No Identifiable Harm
3. Minor adverse effect, completely resolved
4. Minor adverse effect, Chronic
5. Major Adverse Effect, completely resolved
6. Major Adverse Effect, Chronic
7. Death

i. Corrective Action Needed

   i. Do not implement.
   ii. Written risk acceptance required.
   iii. Executive notification required.
   iv. Fix or remove from use within 24 hours.
   v. Fix or remove from use within 72 hours.
   vi. Fix or remove from use within 1 month.
   vii. Fix or remove from use within 6 months.
   viii. No corrective action feasible.
   ix. No corrective action needed.
j. Completeness of Actual Fix
   i. None needed
   ii. Partial
   iii. Complete
   iv. None Feasible
k. Steps taken
   i. Software Upgrade (vendor)
   ii. Training for local IT
   iii. Configuration Change (local IT)
   iv. Custom Programming (local IT)
   v. IT Change Control improved
   vi. Care Process Change
   vii. Policy Change
   viii. Training for End Users